Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] A smartcard transaction system configured with a biometric security system, said system comprising:
a smartcard configured to communicate with a reader;
a reader configured to communicate with said system;
a biometric sensor configured to detect a proffered biometric sample, said biometric sensor configured to communicate with said system; and,
a device configured to verify said proffered biometric sample to facilitate a transaction.

[c2] The smartcard transaction system of claim 1, wherein said sensor is configured to communicate with said system via at least one of a smartcard, a reader, and a network.

[c3] The smartcard transaction system of claim 1, wherein said biometric sensor is configured to facilitate a finite number of scans.

[c4] The smartcard transaction system of claim 1, wherein said biometric sensor is configured to log at least one of a detected biometric sample, processed biometric sample and stored biometric sample.

[c5] The smartcard transaction system of claim 1, further including a database configured to store a data packet, wherein said data packet includes at least one of proffered and registered biometric samples, proffered and registered user information, terrorist information, and criminal information.

[c6] The smartcard transaction system of claim 5, wherein said database is contained in at least one of the smartcard, smartcard reader, sensor, remote server, merchant server and smartcard system.

[c7] The smartcard transaction system of claim 6, wherein said remote database is configured to be operated by an authorized sample receiver.

[c8] The smartcard transaction system of claim 1, further including a device configured to compare a proffered biometric sample with stored biometric sample.

[c9] The smartcard transaction system of claim 8, wherein said device is configured to compare at least one characteristic of a biometric sample including at least one of minutia, vascular patterns, prints, waveforms, odorants, nodal points, reference points, size, shape, thermal patterns, blood flow, and body heat.

[c10] The smartcard transaction system of claim 8, wherein said device configured to compare a biometric sample is at least one of a third-party security vendor device and local CPU.

[c11] The smartcard transaction system of claim 8, wherein a stored biometric sample comprises a registered biometric sample.

[c12] The smartcard transaction system of claim 11, wherein a registered biometric sample is associated with at least one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

[c13] The smartcard transaction system of claim 12, wherein different registered biometric samples are associated with a different one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

[c14] The smartcard transaction system of claim 12, wherein a biometric sample is primarily associated with first user information, wherein said first information comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and wherein a biometric sample is secondarily associated with second user information, wherein said second user information comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and wherein said second user information is different than said first user information.

[c15] The smartcard transaction system of claim 1, wherein said smartcard transaction system is configured to begin authentication upon verification of said proffered biometric sample.

[c16] The smartcard transaction system of claim 1, wherein said smartcard is configured to deactivate upon rejection

of said proffered biometric sample.

[c17] The smartcard transaction system of claim 1, wherein said sensor is configured to provide a notification upon detection of a sample.

[c18] The smartcard transaction system of claim 1, wherein said device configured to verify is configured to facilitate at least one of access, activation of a device, a financial transaction, and a non-financial transaction.

[c19] The smartcard transaction system of claim 1, wherein said device configured to verify is configured to facilitate the use of at least one secondary security procedure.